

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the
District of New Mexico

FILED
United States District Court
Albuquerque, New Mexico
Mitchell R. Elfers
Clerk of Court

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

INFORMATION ASSOCIATED WITH (575) 419-0643 IS
STORED AT PREMISES CONTROLLED BY VERIZON
COMMUNICATIONS, INC.

Case No. **23 MR 1550**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the _____ District of New Mexico, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 1153	Offenses committed in Indian Country
18 U.S.C. § 1111	First Degree Murder

The application is based on these facts:

See attached affidavit, incorporated herein by reference.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Alyson Berry, Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
Telephonically Sworn and Electronically Signed (specify reliable electronic means):



Date: August 14, 2023

Judge's signature

City and state: Farmington, New Mexico

B. Paul Briones, United States Magistrate Judge
Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO**

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
(575) 419-0643 STORED AT PREMISES
CONTROLLED BY VERIZON
COMMUNICATIONS, INC.

Case No. _____

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Special Agent Alyson Berry, having been duly sworn, do hereby depose and say:

INTRODUCTION AND AGENT BACKGROUND

1. I make this Affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises owned, maintained, controlled, or operated by Verizon Communications, Inc., a telecommunications provider headquartered at 1095 Avenue of the Americas, New York, New York, 10036. The information to be searched is described in the following paragraphs and in Attachment A. This Affidavit is made in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. §§ 2703(c)(1)(A) to require Verizon Communications, Inc. to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the account, including the contents of communications.

2. I am a Special Agent with the Federal Bureau of Investigation and have been since July 2020. I am currently assigned to the Albuquerque Division of the FBI, Farmington Resident Agency, and have primary investigative responsibility for crimes that occur in Indian Country, including violent crimes such as homicide, robbery, aggravated assault, and child sexual assault. In 2021, I attended an advanced Indian Country Crime Scene Investigation

course, including techniques for evidence collection and best practices for homicide investigations.

3. The facts in this Affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This Affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this Affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1153 and 1111, First Degree Murder in Indian Country, have been committed by Justin Puerto (hereinafter referred to as PUERTO) and possible other unknown persons. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), and (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

TECHNICAL INFORMATION REGARDING VERIZON COMMUNICATIONS, INC.

6. In my training and experience, I have learned that Verizon Communications Inc. (“Verizon”) provides communications, technology, information and entertainment products and services to businesses, consumers and government agencies. The company offers voice, data and video services and solutions through its wireless and wireline networks.

7. Based on conversations with other law enforcement officers with experience in

executing and reviewing search warrants of mobile telephone accounts, I learned that search warrants for such accounts have revealed stored files sent and/or received many years prior to the date of the search.

8. In general, telecommunication providers like Verizon ask each of their subscribers to provide certain personal identifying information when registering for an account. This information could include the subscriber's full name, physical address, e-mail address and means and source of payment (including any credit or bank account number).

9. Telecommunication providers typically retain certain transaction information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in to services (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as the device used to log into the account, and other log files that reflect usage of the account. In addition, providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access content on the account.

10. In my training and experience, evidence of who was using a device may be found in address books, contact or buddy lists, e-mail in the account, and information associated with pictures and files.

11. In my training and experience, I have learned that VERIZON is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information

about the locations of the cellular telephones to which they provide service, including E-911 Phase II data, also known as GPS data or latitude-longitude data and cell-site data, also known as “tower/face information” or cell tower/sector records. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device’s signal using data from several of the provider’s cell towers. Cell-site data identifies the “cell towers” (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the “sector” (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data is typically less precise than E-911 Phase II data.

12. Based on my training and experience, I know that VERIZON can collect E-911 Phase II data about the location of the Target Cell Phone, including by initiating a signal to determine the location of the TARGET DEVICE on VERIZON’s network or with such other reference points as may be reasonably available.

13. Based on my training and experience, I know that VERIZON can collect cell-site data about the TARGET DEVICE. Based on my training and experience, I know that for each communication a cellular device makes, its wireless service provider can typically determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer connected at the end of the communication; and (5) the duration of the communication. I also know that wireless providers such VERIZON typically collect and retain

cell site data pertaining to cellular devices to which they provide service in their normal course of business in order to use this information for various business-related purposes.

TECHNICAL TERMS

14. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include capabilities as described in other stand-alone devices listed below, including features of a digital camera/video recorder, portable media player, PDA, GPS, and internet.
- b. Digital camera/video recorder: A digital camera/video recorder is a camera that records pictures as digital picture files and has the capability of video recording

events. Digital cameras/video recorders use a variety of fixed and removable storage media to store their recorded images and video files. Images and video files can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras/ video recorders also include a screen for viewing the stored images and videos. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. Portable media player: A portable media player (or “MP3 Player”) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include

various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

- e. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international

borders, even when the devices communicating with each other are in the same state.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

15. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

16. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the TARGET DEVICE because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

17. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Target Device consistent with the warrant. The examination of the Target Device may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Target Device to human inspection in order to determine whether it is evidence described by the warrant.

DETAILS OF INVESTIGATION

18. The United States, including FBI, is conducting a criminal investigation of PUERTO, and others regarding possible violations of 18 U.S.C. §§ 1153 and 1111, First Degree Murder in Indian Country.

19. On August 7, 2023 at approximately 6:00 p.m., the Jicarilla Apache Police Department (JAPD) responded to a report of shooting on East Side Street in Dulce, New Mexico, which is located on the Jicarilla Apache Reservation. I am informed by a JAPD Criminal Investigator (CI), that he reported to the location and found the deceased body of the victim (hereinafter referred to as JOHN DOE), year of birth 2007, lying in the street with seven spent .40 caliber shell casings around JOHN DOE's body. Upon further examination, the JAPD CI observed multiple entry and exit wounds on JOHN DOE's body that appeared to be bullet holes. Based on his training and experience, JAPD CI believed JOHN DOE was murdered by gunfire and treated the incident as a homicide.

20. Through a joint investigation by JAPD and the FBI, I learned that JOHN DOE's family members and residents of Dulce believed an individual named Justin Puerto (hereinafter referred to as PUERTO), year of birth 2008, was responsible for the possible murder of JOHN DOE. At approximately 11:00 p.m., JAPD received a tip that PUERTO was presently at 16 Ornate Street in Dulce, the residence of his girlfriend (hereinafter referred to as H.L.), year of birth 2007, and H.L.'s mother (hereinafter referred to as M.L.). Shortly thereafter, JAPD and the FBI went to 16 Ornate Street and JAPD apprehended PUERTO.

21. Based on PUERTO's date of birth, I believed he was approximately 15 years old at the time of the crime and of the interview. PUERTO said he lived with his grandmother (hereinafter referred to as L.W.), year of birth 1957. W.L. stated she is PUERTO's legal guardian. On August 8, 2023 at approximately 12:03 a.m., PUERTO was provided his Miranda Warnings in the presence of L.W. He stated that he understood his rights and agreed to speak with law enforcement. PUERTO stated that he was friends with JOHN DOE and that he heard from multiple sources that JOHN DOE had been killed on the evening of August 7, 2023.

PUERTO stated that prior to the murder he was with his older brother Travis Begaye Jr. (hereinafter referred to as BEGAYE), year of birth 2004, hiking on the reservation. After finishing the hike, PUERTO and BEGAYE were walking back and heard nearby gunshots. PUERTO and BEGAYE ran away from the sound of gunshots and went to a family member's house. Eventually, PUERTO and BEGAYE managed to get back to L.W.'s house. On August 7, 2023 at approximately 7:30 p.m., PUERTO called his girlfriend, H.L. and arranged to have her mother, M.L., pick PUERTO up from his residence and take him to her residence at 16 Ornate Street.

22. On August 8, 2023 at approximately 12:45 a.m., FBI spoke with BEGAYE in the vicinity of 16 Ornate Street. BEGAYE's date of birth is December 15, 2004, meaning he was 18 years old at the time of the interview. During the conversation, BEGAYE stated that he heard JOHN DOE was dead and BEGAYE knew that JOHN DOE and PUERTO were close friends. BEGAYE said he tried to see and speak with PUERTO early in the day on August 7, 2023, but PUERTO's vibe seemed off. BEGAYE said that he did not see PUERTO on August 7, 2023, and that he did not go on a hike with PUERTO. BEGAYE further stated that on August 7, 2023, he received three Instagram voice calls from PUERTO around the time that PUERTO said they were on a hike together. BEGAYE does not currently have a telephone, but PUERTO was able to contact BEGAYE through BEGAYE's girlfriend's cellular telephone. During the first call, PUERTO told BEGAYE that he had a plan to make some money. During the second call, PUERTO told BEGAYE that PUERTO successfully made money that afternoon. During the third call, PUERTO called BEGAYE said he had "fucked up." BEGAYE stated that PUERTO sounded like he was crying during the phone call and was questioning whether what happened

was worth the money he made. BEGAYE believed that PUERTO was in some way involved in the murder of JOHN DOE.

23. On August 8, 2023, after speaking with BEGAYE, FBI and JAPD CI interviewed H.L. in the vicinity of 16 Ornate Street. H.L. was 15 years old at the time of the interview and her mother, M.L., consented to the interview. H.L. stated that on August 7, 2023 around 7:30 p.m., PUERTO contacted H.L. by cellular telephone and asked to come to H.L.'s house. H.L. confirmed that PUERTO's cellular telephone number is (575) 419-0643, the TARGET DEVICE.

24. On August 8, 2023 after speaking with H.L., FBI requested the TARGET DEVICE from PUERTO for evidentiary purposes. PUERTO stated that the TARGET DEVICE was lost and that he's been using Instagram to voice call people or he used H.L.'s cellular telephone. PUERTO then opened H.L.'s cellular telephone and showed the recent call history to FBI. There appeared to be calls between H.L. and PUERTO's contact, which was saved as "Justin" with a blue heart symbol, as recently as August 7, 2023. H.L. and M.L. consented to the FBI taking custody of H.L.'s cellphone telephone and examining the contents of the cellular telephone.

25. Also on August 8, 2023, JOHN DOE's friend (hereinafter referred to as E.L.), year of birth 2006, was interviewed by law enforcement. E.L. stated PUERTO walked up to him during school on the day of the incident and said, "I'm gonna make my mark today". E.L. believed that statement meant PUERTO was going to kill someone. After school PUERTO walked up to E.L. and JOHN DOE and arranged to make "a deal" after school. E.L. stated both PUERTO and JOHN DOE sold illegal drugs and the deal PUERTO made with JOHN DOE was for \$600 and some vapes. E.L. believed PUERTO was acting weird and told JOHN DOE not to do the deal with PUERTO. E.L. believed PUERTO was jealous of JOHN DOE. At

approximately 4:30 p.m. E.L. and JOHN DOE hung out after. E.L. left for football practice and JOHN DOE went to go meet PUERTO for their arranged deal. When E.L. arrived home later that night, he heard about the shooting incident and immediately believed PUERTO killed JOHN DOE. E.L. confirmed JOHN DOE used Instagram to communicate with other classmates including him and PUERTO. E.L. provided JOHN DOE's Instagram handle as "85.136rs" and PUERTO's Instagram handle as "gfolks". E.L. stated PUERTO had multiple Instagram accounts and changed them often.

26. On August 9, 2023 Dulce High School Administration notified JPDCI they were conducting an internal investigation into multiple statements received by students that PUERTO had threatened them on Thursday and Friday of the week before (August 3 and 4, 2023). One student (hereinafter referred to as D.L.T.), year of birth 2006, stated PUERTO told him, "You better watch your back or this 40 is gonna bite you." PUERTO gestured with his hand and finger signifying a gun. Later, PUERTO passed D.L.T. in the hallway and said, "You better watch this forty and quit acting like a bitch and keep walking." Another student (hereinafter referred to as D.J.T.), year of birth 2007, stated PUERTO approached him at school and pointed a finger in D.J.T.'s face and said, "tell your brother he better watch out for that forty." D.L.T. and D.J.T. are brothers.

27. H.L. was interviewed a second time on August 11, 2023, by FBI. It was learned H.L. filmed an Instagram video of PUERTO near River Road Platform shooting the firearm a week prior to the shooting incident. H.L. utilized her cellular device to film the video and upload the video to her Instagram account. H.L. was also PUERTO had in his possession a black handgun (make and model unknown) and PUERTO kept the handgun in a dark colored duffle bag. H.L. also disclosed PUERTO came over to her residence the evening after the incident and while in H.L.'s bedroom, PUERTO told H.L. he "did it." H.L. believed PUERTO was referring to the shooting incident and death of JOHN DOE which occurred earlier that day.

28. FBI executed a search warrant on PUERTO's residence on August 11, 2023.

Within the evidence items collected, an Apple iPhone was seized. The device likely belongs to PUERTO, as it was with PUERTO's belongings in his closet. Among the items were identifying belongings of PUERTO's, including his wallet, social security card, and identification. The iPhone was disabled, which is an indication it may have been restored back to factory settings from a remote location.

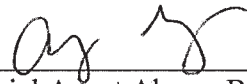
29. Based on my training and experience, I know it is not uncommon for juveniles that have committed violent crimes to discuss their motivations, plans, and actions with others via text messaging, phone calls, or social media. PUERTO used social media to advertise the fact that he owned a firearm. It is additionally feasible he communicated with his friends, family, or classmates before and after the shooting incident. Admissions by H.L. disclosed she and PUERTO communicated with their cell phones regularly. The contents of the phone may also provide information to determine the whereabouts of the weapon currently.

CONCLUSION

25. Based on the forgoing, I request that the Court issue the proposed search warrant.

26. Assistant United States Attorney Alexander Flores has reviewed and approved this application.

27. I swear that this information is true and correct to the best of my knowledge.



Special Agent Alyson Berry
Federal Bureau of Investigation

Electronically SUBSCRIBED and telephonically SWORN to
me this 14 day of August, 2023.



THE HONORABLE B. PAUL BRIONES
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with mobile telephone number (575) 419-0643 that is stored on servers owned, maintained, controlled, or operated by Verizon Communications, Inc. a company headquartered in New York, New York, including information located on servers that are not physically located within the United States but which are nonetheless owned, maintained, controlled or operated by Verizon Communications, Inc.

Verizon Communications, Inc. shall disclose responsive data, if any, by sending to Special Agent Alyson Berry, 215 West Elm Street, Farmington, New Mexico, 87401 using the US Postal Service or another courier service, or electronic communication via amberry2@fbi.gov.

ATTACHMENT B
Particular Things to be Seized

I. Information to be disclosed by Verizon Communications, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Verizon Communications, Inc., regardless of whether such information is stored, held, or maintained inside or outside the United States, and including any information of any nature that has been deleted but is still available to Verizon Communications, Inc., is required to disclose the following information to the United States for the accounts or identifiers listed in Attachment A, from July 24, 2023 to the present:

a. Account Information – Subscriber name, addresses associated with this account, primary email address, secondary email addresses, connected applications and sites, and account activity from the time of the account’s creation to present including account sign in locations, browser information, platform information, account status, and internet protocol (IP) addresses;

b. Phone Information - Device make, model, and International Mobile Equipment Identifier (IMEI) of all associated devices linked to the Verizon accounts of the TARGET DEVICE;

c. Evidence of user attribution - accounts, email accounts, passwords, PIN codes, account names, user names, screen names, remote data storage accounts, credit card number or other payment methods, contact lists, calendar entries, text messages, voice mail messages, pictures, videos, telephone numbers, mobile devices, physical addresses, historical GPS locations, two-step verification information, or any other data that may demonstrate attribution to a particular user or users of the account(s).

d. Calendar - All calendars, including shared calendars and the identities of those with whom they are shared, from July 24, 2023 to the present, calendar entries, notes, alerts, invites, and invitees;

e. Contacts - All contacts stored by Verizon including name, all contact phone numbers, emails, social network links, and images;

f. Documents – All user created documents stored by Verizon,

g. E-mail - All email messages from the time of the account's creation to present, including by way of example and not limitation, such as inbox messages whether read or unread, sent mail, saved drafts, chat histories, and emails in the trash folder. Such messages will include all information such as the date, time, IP Address routing information, sender, receiver, subject line, any other parties sent the same electronic mail through the 'cc' (carbon copy) or the 'bcc' (blind carbon copy), the message content or body, and all attached files;

h. Photos - All images, graphic files, video files, and other media files stored in the device;

i. Location History - All location data whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, and precision measurement information such as timing advance or per call measurement data, and Wi-Fi location. Such data shall include the GPS coordinates and the dates and times of all location recordings;

j. App Purchases - All applications downloaded, installed, and/or purchased by the associated account and/or device;

k. Search History - All search history and queries from the time of the account's creation to present, including by way of example and not limitation, such as World Wide Web (web), images, news, shopping, ads, videos, maps, travel, and finance;

l. Voice - All call detail records, connection records, short message system (SMS) or multimedia message system (MMS) messages, and voicemail messages sent by or from the Verizon account associated with the target account/device;

m. Wallet/Checkout - All information contained in the associated account including transactions, purchases, money transfers, payment methods, including the full credit card number and/or bank account numbers used for the transactions, and address book;

n. Cloud – All live and deleted files stored in the listed user's Cloud;

o. A list of linked accounts based upon IP address and session cookie;

p. The types of services utilized;

q. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

r. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

II. Information to be seized by the government

1. All information described above in Section I, including correspondence, records, documents, photographs, videos, electronic mail, chat logs, and electronic messages, that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 1153 and 1111, First Degree Murder in Indian Country, for each account or identifier listed on Attachment A.

2. Credit card and other financial information, including but not limited to bills and payment records;

3. Evidence of the identity of who used, owned, created, or controlled the accounts or identifiers listed on Attachment A, including records that could help reveal the whereabouts of such person(s);

4. Evidence of the times the accounts or identifiers listed on Attachment A was used;
5. Evidence indicating the electronic account owner's state of mind as it relates to the crimes under investigation;
6. Evidence of any coconspirators, accomplices, and aiders and abettors in the commission of the above offenses;
7. Passwords and encryption keys, and other access information that may be necessary to access the accounts or identifiers listed on Attachment A and other associated accounts;
8. All communications between the accounts or identifiers listed on Attachment A.